Navigator

Industrial Cybersecurity Outlook 2023-2030

TXOne Networks

navigator.westlandsadvisory.com

Macro Trends underpinning greater OT cybersecurity investment remain strong

Despite challenging global economic conditions, expenditure on OT cybersecurity has continued to increase. There are 3 investment drivers: digital transformation, regulation, and risk management.

The growing interconnectivity among OT devices, systems, and processes has facilitated the digital transformation of industrial operations, increasing demand for cloud computing services, data analytics, digital twins, and machine learning. Convergence between IT and OT has further accelerated this trend, facilitating seamless integration and data exchange between two previously isolated environments. The new digital asset owner is characterised by higher levels of interoperability and collaboration, enabling process optimisation and productivity gains. The benefits of digital transformation need to be managed alongside the increased exposure to IT & OT vulnerabilities, requiring new cybersecurity policies, processes, and procedures to ensure the resilience of future operating models.

Regulation continues to influence procurement decisions. Enforcement efforts are strengthening, regulation is expanding to cover more industry sectors and supply chains, and there is a growing requirement for higher levels of resilience. Examples in the United States include both CISA's Binding Operational Directive 23-01 and TSA Directive SD 1580/82-2022-01 which became enforceable in 2023, and OMB M-22-09 focus on establishing Zero Trust in Federal operated infrastructure. The NIS 2 directive will be enforceable in each EU country from 2024 and now includes key manufacturing sectors, increasing coverage from 21% to 36% of the EU's economic base, whilst the Critical Entities Resilience Act (CER) covers critical infrastructure. Australia, India, Japan and Canada have all recently launched new regulation or are in the process of reviewing the current status.

The final contributing factor to increased investment is heightened executive awareness of OT risk due to widely reported ransomware incidents impacting industry peers. This has resulted in improved governance and a focus on cybersecurity resilience. Research from Orange Cyberdefense highlights that the manufacturing sector was the most attacked industry sector in 2022, due in part to its large size, and from an attacker perspective its relative attractiveness (manufacturing CVSS scores are 33% higher than the global average). It also highlights that 58% of incidents result from internal errors and misconfigurations. Asset owners need to protect again external threat but also closely monitor internal processes.

Evolving Cybersecurity Requirements

The responsibility for OT cybersecurity differs by organisation. It may be the Operations team, the Engineering Director or the CISO. For simplicity we refer to the team responsible for OT cybersecurity as OT Security Leaders.

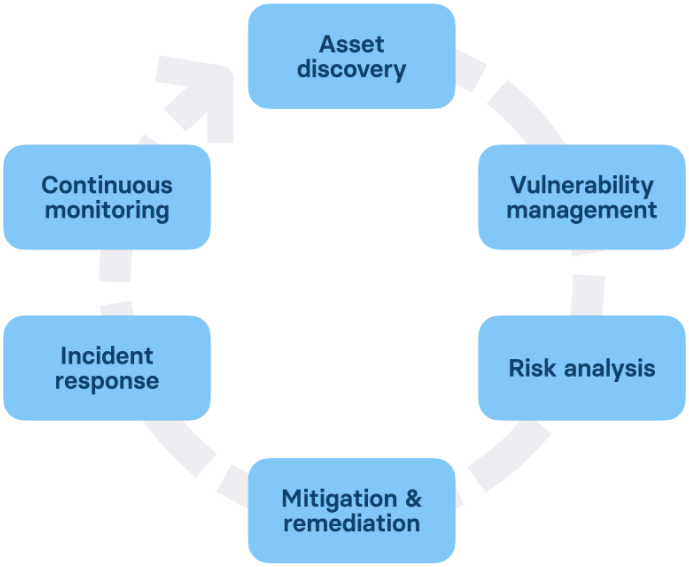
The primary goal of OT Security Leaders it to ensure that the risk of a cyber incident impacting the Reliability, Availability and Safety of operations is minimised. This requires identification and management of vulnerabilities, and a layer of controls to prevent threat actors from accessing networks. The logical starting point is to identify and classify all assets though this is rarely a simple task. Plants may be 30 years old with no official asset register and reliant on a patchwork of different OEM systems and sensors. Security Leaders need to have visibility of the assets they are managing, the firmware and patch status of those assets, and what they are connecting to.

Once assets are identified and logged, OT Security Leaders should address vulnerabilities that are known and understood and implement processes to continually monitor and manage them. This may include changing default passwords, implementing patch management, and monitoring of access controls.

Defence-in-Depth (DiD) is the traditional layered security model applied to OT environments and comprises a series of technical and administrative controls to protect data, applications, endpoints and the network. This makes it more difficult for adversaries to move laterally, preventing them from exploiting vulnerabilities. Technical controls include firewalls at the IT/OT network boundary and between zones to ensure appropriate segmentation, endpoint protection, and access control. OT network monitoring provides an additional layer, detecting anomalies and automating response.

However, as networks converge and data exchange between the factory floor and the cloud expands, so does the scope of the threat. DiD alone is not sufficient to protect OT operations. Modern organisations require a security approach that enforces policy, monitors, and orchestrates across a complex network of digital infrastructure, entities and physical assets.

The principle of Attack Surface Management (ASM) helps to address the challenge of identifying, assessing, and mitigating the vulnerabilities that exist within an organisation's digital and physical infrastructure, and external entities including supply chain and OEM partners.



ASM focusses on identifying and managing risks through a proactive approach to security management, whereas DiD is focused on the layering of controls to protect against threats. The approaches are entirely complementary as noted in NIST 800-53 which describes Attack Surface reduction as being *"aligned with threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organisations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services."* A layered defence is recommended as part of the overall security architecture alongside a 'least privilege' approach to managing network access.

ASM is increasingly being implemented by OT Security Leaders. This includes asset discovery, risk assessment and remediation. It should also include OT specific response plans built on an understanding of the Tactics, Techniques and Procedures (TTP's) that can be unique to the industrial sector.

A strong OT security posture requires technical controls to be interoperable. The firewalls, IDS, antivirus, and access control solutions deployed in the DiD framework should integrate and exchange data, enabling orchestration of security processes and workflows to improve threat detection and incident response. This also includes the components of ASM, providing OT Security Leaders with a unified and automated security operation.

Security Vendor Selection

There is no single vendor that provides native capabilities covering all technical security controls. OT Security Leaders planning to implement a new security program, consolidate vendors, or refresh its security program should look towards a platform approach, ensuring that vendor solutions can integrate. An advantage of using a single platform is that it shifts the integration burden to the platform vendor. The platform vendor becomes responsible for making sure that their products interoperate, thereby reducing the burden of technology debt that the Asset Owner takes on.

The ecosystem consists of two main vendor categories. OT Network Protection vendors typically provide firewalls, including coverage of industrial protocols, and a range of additional capabilities from endpoint protection to SOCaaS. The main use cases include network protection, segmentation and access management, but many also offer visibility solutions. Most vendors also have a strong IT security platform, enabling industrial enterprises to manage IT and OT security operations separately or to merge them into a single operation.

Asset Visibility and Threat Management vendors provide visibility, vulnerability management, and threat detection supported by OT specific threat intelligence. These vendors typically provide products for OT ASM though each vendor has its own unique strength, ranging from deployment type, managed services or capability (remote access management, incident response etc.)

The following vendors, reviewed in WA's latest analysis of the OT Cybersecurity Industry, provide platform solutions and integrations and should be considered by Security Leaders.

When selecting vendors OT Security Leaders should also consider a vendors' strategic direction. WA analysts noted significant innovation across the industry over the last 18 months, and the technical roadmaps of some vendors are particularly strong, including improvements to platform usability, new integrations, refinements to risk analytics, and new OT use cases.

Profile: TXOne Networks

Summary

The TxOne product portfolio includes three distinct offerings for network protection.

- Security Inspection which is a set of portable products for malware scanning.
- Endpoint Protection through Stellar, an on-prem, agent based solution managed through a centralised management console. Use cases include AV, asset visibility, industrial application control and patch management.
- Network Defense which includes EdgeIPS and EdgeFire OT security appliances. Use cases include network visibility, segmentation and virtual patching. EdgeFire 2.0, released in May 2023, includes VPN support and increased protocol analysis and control.

Positioning

TXOne's vision is to provide asset operators with a unified view of the OT network, providing context and increasing levels of orchestration to both security and operational teams. Currently EdgeOne is the industrial central management console for monitoring OT networks and provides an insight into the future direction of the company. The product integrates with Trend Micro Vision One (XDR) to provide both IT and OT network visibility for industrial manufacturers looking to consolidate security infrastructure and centralise visibility across its operations. EdgeOne integrates TXOne's Threat Intelligence, improving administration and OT protocol management, and provides a visual of the IT/OT network map.

The company's solutions are supported by a strong Threat Intelligence service. Insight is created through combining TXOne's intelligence with endpoint, network and 3rd party sources and is shared with the wider OT research community. The company has discovered over 30 ICS related CVE's.

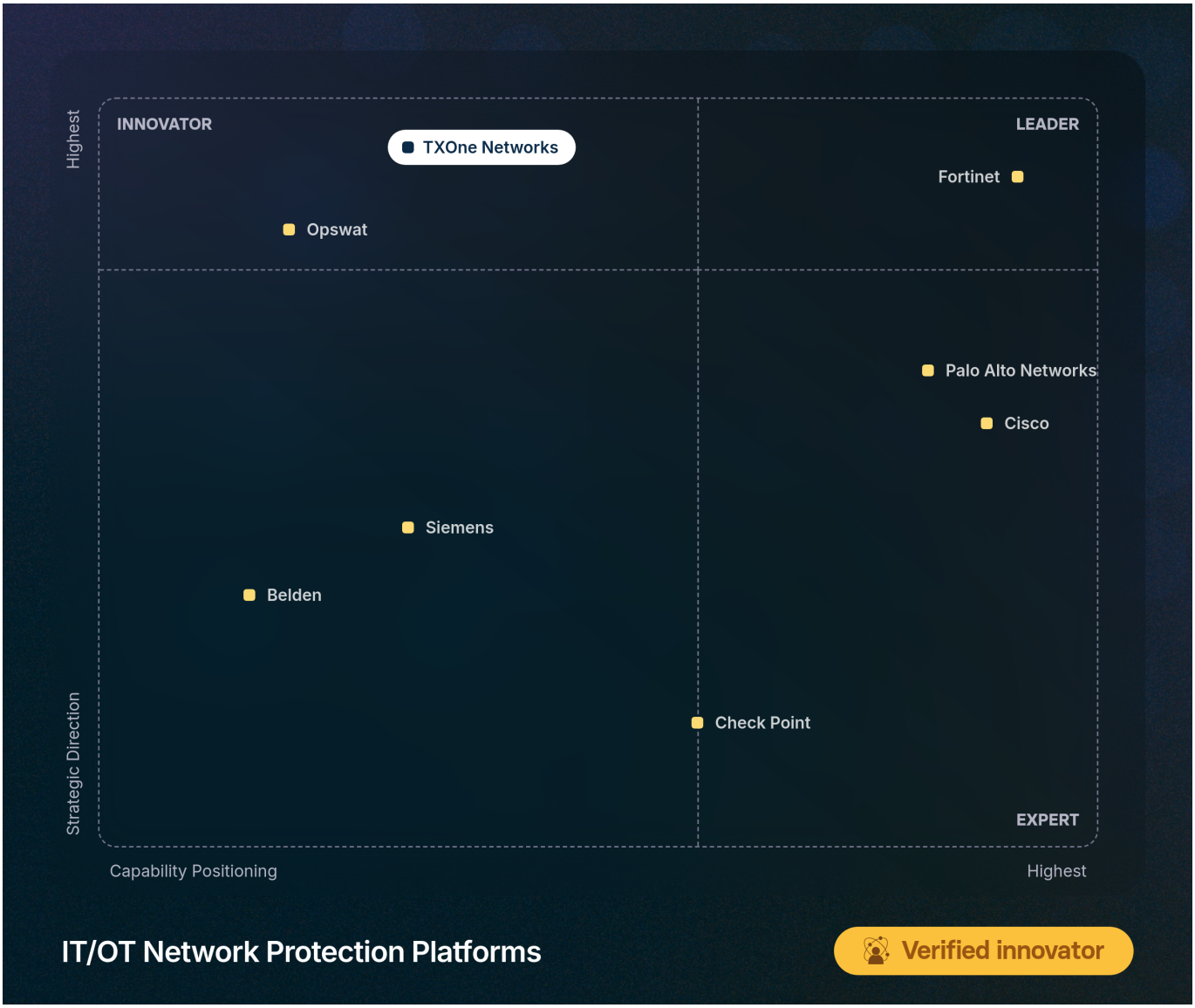
TXOne's channels to market include OEM relationships, Trend Micro, and OT partners. Co-innovation and OEM integration is central to the company strategy and the company will continue to focus on building its alliance network.

The company has deep OT expertise including strong vertical market expertise in semiconductor and automotive manufacturing sectors and with critical infrastructure providers (energy, Oil & Gas)

Known for

- Strong customer base in APAC, particularly Japan
- Trend Micro Partnership
- OEM innovations and collaborations
- OT sector expertise with notable strength in semiconductor and automotive

IT/OT Network Protection Platforms



OT Network Protection is integral to a Defence-in-Depth approach, providing protection at the network boundary through network monitoring and enforcement of policies.

Definition

Network Protection platforms have several native capabilities, including firewalls and access control. Use-cases may include network visibility, segmentation, Zero Trust policy enforcement, and incident response. Most network protection platforms also include other native technical controls (e.g. endpoint protection) or integrate with third party tools. The Platform orchestrates and provides centralised visibility and control of OT cybersecurity operations.

Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”.

Evaluation

The following capabilities are included in the evaluation:

- Network Protection including Firewalls, IPS, unidirectional gateways and data didoes.
- Network Segmentation including Firewalls, VLAN's, Access Control Lists (ACL), SDN and agentless Micro Segmentation through identification and logical grouping of assets and devices.
- Endpoint Protection including malware scanning, application whitelisting and patch management, and USB protection.
- Secure Access including PAM, VPN and ZTNA.
- Security Operations & Incident Response including SIEM, SOAR, XDR and EDR plus playbooks.

Qualification

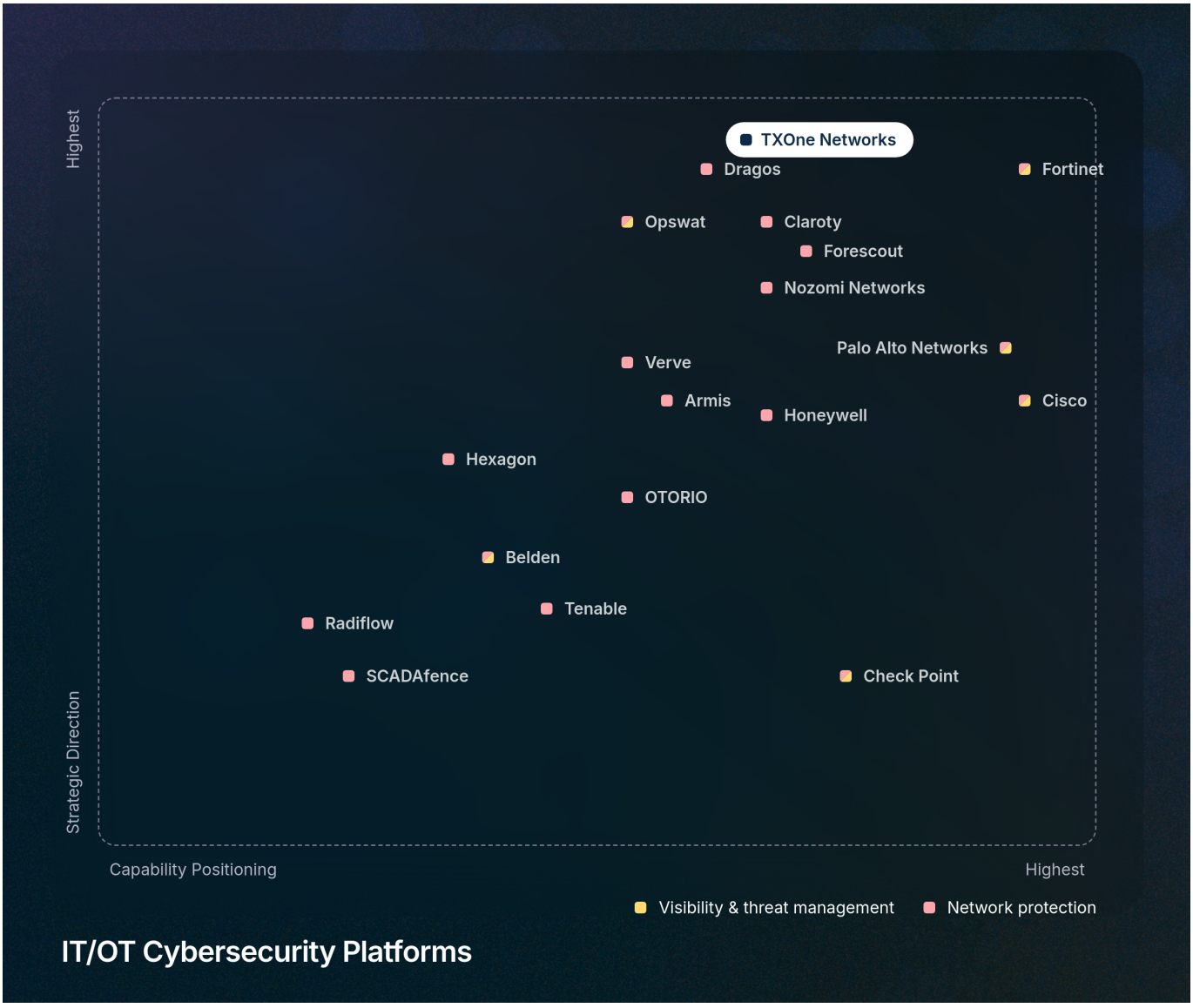
Competitors must meet the following criteria to qualify for consideration in the IT/OT Network Protection Platform Navigator:

- Company must provide native solutions for OT network protection including all or one of NGFW, IPS and Data Diode.
- The relevant products integrate into a centralised platform with other network protection products including access management.
- The platform ingests information from other platforms or sources to enrich the data and provide context.
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations, providing network and device visibility and management.
- The platform has SIEM capabilities or integrates with SOAR platforms.
- The company has strong coverage in more than one geographical region.

Methodology

Further information on WA's methodology can be found on the website at https://navigator.westlandsadvisory.com

IT/OT Cybersecurity Platforms



IT/OT Cybersecurity Platforms include several native products and integrate with other products or platforms to provide the customer with a single, unified view of operations.

Definition

The market consists of two types of vendors, those providing Visibility & Threat Management and those that have a strong Network Protection product portfolio. Security Leaders will usually rely on at least one vendor from each category. However, competitors

are expanding capabilities and it is increasingly common for vendors to provide both Visibility & Threat Management and Network Protection solutions.

Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”.

Evaluation

The following technologies are included in the evaluation:

- Asset Visibility
- Network Protection
- Network Segmentation
- Vulnerability Management
- Risk Management
- Endpoint Protection
- Secure Access
- Threat Detection
- Security Ops & IR
- Back-up & Recovery

Qualification

Competitors must meet the following criteria to qualify for consideration in the IT/OT Cybersecurity Platform Navigator:

- The company has native solutions in at least 4 technology categories.
- The relevant products integrate into a centralised platform.
- The platform ingests information from other platforms or sources to enrich the data.
- The platform has a sophisticated central management function that provides analytics and reporting for analysts to monitor and manage security operations.
- The platform has SIEM capabilities or integrates with SOAR platforms.

- The company has strong coverage in more than one geographical region.

Methodology

Further information on WA's methodology can be found on the website at https://navigator.westlandsadvisory.com

Concluding

OT networks are often Data Rich and Information Poor with huge benefits yet to be derived from greater data exploitation. To accelerate digital transformation, Asset Owners require asset and network visibility but also need to manage the data and alerts efficiently. This has resulted in innovation to not only identify assets, but to also categorise, profile and automate risk and vulnerability management. Asset discovery and vulnerability management are high growth product segments and address the 'known known' risks to operations. Alongside firewalls and network segmentation, access management, and endpoint protection, these controls provide strong protective measures.

There is a growing requirement in regulation and standards to ensure that the 'unknowns' are covered requiring continuous monitoring through either passive or active scanning to detect and alert if there are deviations from the baseline. To protect against the unknown scenarios, asset owners should move towards implementing a security model based on resilient operations and a focus on people, technology and processes to ensure organisations are able to withstand and recover from a cyber incident with minimal disruption to operations. ASM is key to getting ahead of threats whilst well documented Incident Response procedures facilitate a co-ordinated, timely and effective response.

By 2030 we expect OT cybersecurity maturity to have advanced significantly within utilities and large, transnational manufacturing organisations. Many organisations will have converged security operations providing company-wide visibility, with dedicated OT teams trained on processes and procedures. Security will be increasingly managed by cloud platforms, either by the asset owners or by a managed service provider, and there will be a growing focus on managing and protecting wireless 5G networks. WA also expects improved supply chain cybersecurity maturity and a greater installed base of industrial operations built on secure-by-design principles. Security Leaders should ensure that they work with partners that have solutions to address current and future industry requirements.